# Towards efficient partial order techniques for time Petri nets

Hanifa Boucheneb

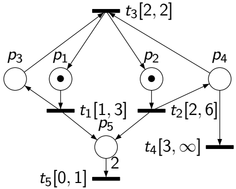
Joint work with K. Wang & K. Barkaoui & Z. Li

*École Polytechnique de Montréal*

October 26, 2020

# Overview

# Time Petri nets (TPN)

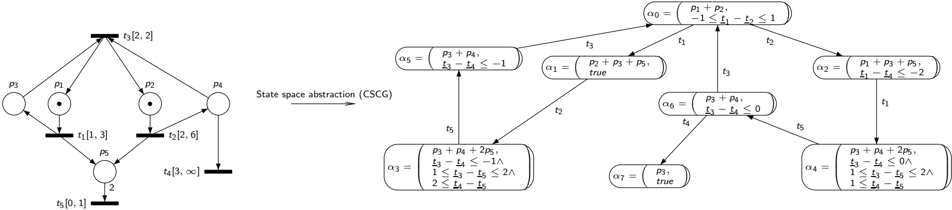



TPN = PN where each $t_i$ has a firing interval $[a_i, b_i]$.

- $[a_i, b_i]$ specifies the minimal and maximal firing delays of $t_i$.
- When $t_i$ is newly enabled, $I(t_i) = [a_i, b_i]$. Bounds of $I(t_i)$ decrease with time, until $t_i$ is fired or disabled.
- $t_i$ is firable, if $\downarrow I(t_i) = 0$. It must fire immediately, when $\uparrow I(t_i) = 0$.
- Its firing takes no time but leads to a new marking.

# Time Petri nets (TPN)

Verification is mainly based on time abstractions:




State space abstractions:

- preserve markings and firing sequences,
- are finite for bounded TPN, but
- suffer from the state explosion problem.

$\Longrightarrow$ Partial order reduction (POR) techniques are well-accepted to tackle this problem.
$\Longrightarrow$ How to use POR techniques in the context of TPN?

# POR techniques

- POR techniques aim to reduce the state space to be explored, by selecting as few as possible the transitions to be fired, while preserving the properties of interest.
- For the deadlock properties, this selection can be performed using:
  - Stubborn sets method [Valmari et al., 1992, 1993, 2011],
  - Persistent sets method [Godefroid et al., 1996] (special case of stubborn sets) or
  - Ample sets [Peled et al., 1993, 1997].

$\Longrightarrow$ Stubborn sets

# POR techniques: Stubborn sets

**Definition (Valmari et al., 1992, 1993, 2011)**

Let $\alpha \in \mathcal{C}$ be a state class and $\mu \subseteq T$. $\mu$ is a stubborn set of $\alpha$, if:

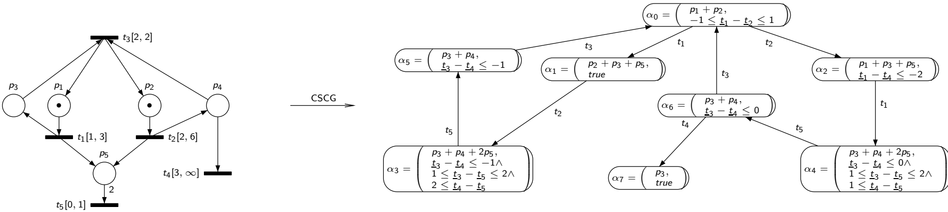
D0: $Fr(\alpha) \neq \emptyset \;\Leftrightarrow\; \mu \neq \emptyset$.

D1w: $\exists t \in \mu, \forall \omega \in (T - \mu)^{+}, \alpha \xrightarrow{\omega} \Rightarrow \; \alpha \xrightarrow{\omega t}$.

D2: $\forall t \in \mu, \forall \omega \in (T - \mu)^{+}, \forall \alpha' \in \mathcal{C}, \alpha \xrightarrow{\omega t} \alpha' \;\Rightarrow\; \alpha \xrightarrow{t \omega} \alpha'$.

- However, the diamond property imposed by D2 is difficult to meet, even for conflict-free transitions.

# POR techniques: Stubborn sets




## Example

For $\alpha_0$, the set $\mu = \{t_1\}$ satisfies:

- $D0$: $Fr(\alpha_0) \neq \emptyset \;\Leftrightarrow\; \mu \neq \emptyset$.
- $D1w$: $\forall \omega \in (T-\mu)^+, \alpha_0 \xrightarrow{\omega} \;\Rightarrow\; \alpha_0 \xrightarrow{\omega t_1}$.
- $D2'$: $\forall \omega \in (T-\mu)^+, \alpha_0 \xrightarrow{\omega t_1} \;\Rightarrow\; \alpha_0 \xrightarrow{t_1 \omega}$.

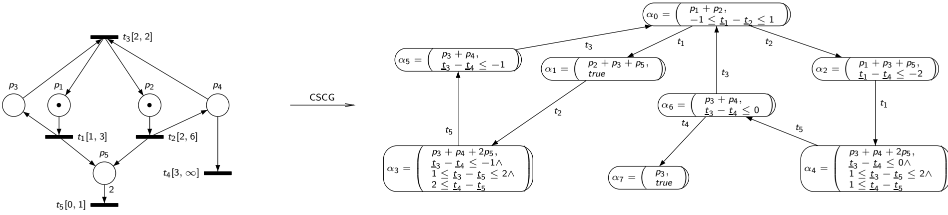
But, it does not satisfy $D2$, since for $t_2$, it holds that:

- $\alpha_0 \xrightarrow{t_2 t_1} \alpha_4$,
- $\alpha_0 \xrightarrow{t_1 t_2} \alpha_3$, and
- $\alpha_3 \neq \alpha_4$ but they share the same marking.

What about using D2' instead of D2?

# POR techniques: Stubborn sets

D0, D1w and D2' are not sufficient to detect deadlocks.




- $\{t_1\} \models_{\alpha_0} D0 \wedge D1w \wedge D2'$ and
- firing $t_1$ from $\alpha_0$ does not allow to detect the deadlock marking $p_3$.

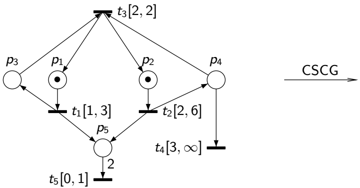
$\Longrightarrow$ D0, D1w and D2' are used in combination with POSETs.

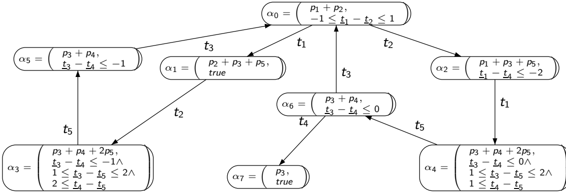
# POR techniques: Stubborn sets with POSETs

- Idea: Relax the firing rule by ignoring some firing order constraints.
- Aim: Compute, by exploring only one sequence, the union of state classes reachable by a set of equivalent sequences (i.e., a POSET).
- Let $\alpha$ be a state class and $\mu \subseteq T$ such that $\mu \models_\alpha D0 \wedge D1w \wedge D2'$. For $t \in \mu \cap Fr(\alpha)$, the successor of $\alpha$ by $t$ is computed without fixing any firing order constraint between $t$ and the transitions outside $\mu$.

Does a POSET cover all state classes reachable by its sequences?

# POR techniques: Limitations of POSETs

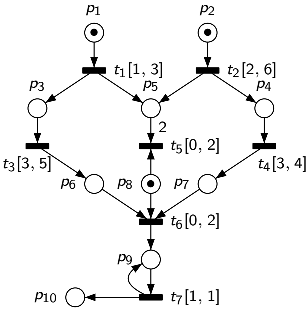


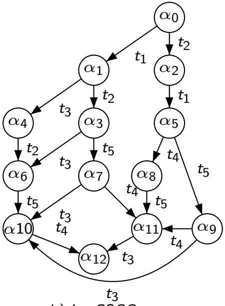

- For $\alpha_0$ and $\mu = \{t_1\}$, the exploration order $t_1 t_2$ of the transitions of the POSET $\{t_1, t_2\}$ will not cover all states of $\alpha_3 \cup \alpha_4 \implies$ the deadlock marking $p_3$ will not be detected.
- For $\alpha_0$ and $\mu = \{t_2\}$, the exploration order $t_2 t_1$ of the transitions of the POSET $\{t_1, t_2\}$ will cover all states of $\alpha_3 \cup \alpha_4 \implies$ the deadlock marking $p_3$ will be detected.

$\implies$ Exploration order of the transitions of a POSET may fail to cover all state classes reachable by its sequences.

$\implies$ Does there always exist an exploration order of the transitions of a POSET that allows to cover all state classes reachable by its sequences?




a) A bounded TPN




b) Its CSCG

- $\alpha_3 = (p_3 + p_4 + 2p_5 + p_8,$
  $-4 \leq \underline{t_3} - \underline{t_4} \leq 2 \wedge$
  $-2 \leq \underline{t_3} - \underline{t_5} \leq 5 \wedge$
  $1 \leq \underline{t_4} - \underline{t_5} \leq 4).$
- $\alpha_5 = (p_3 + p_4 + 2p_5 + p_8,$
  $-1 \leq \underline{t_3} - \underline{t_4} \leq 3 \wedge$
  $1 \leq \underline{t_3} - \underline{t_5} \leq 5 \wedge$
  $0 \leq \underline{t_4} - \underline{t_5} \leq 4).$

c) $\alpha_3 \cup \alpha_5 \neq \alpha_3 \sqcup \alpha_5$

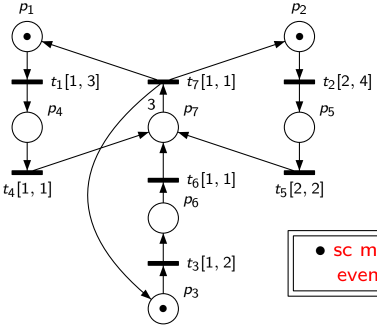
- For $\alpha_0$ and $\mu = \{t_2\}$ (or $\mu = \{t_1\}$), none of the exploration orders of the transitions of the POSET $\{t_1, t_2\}$ allows to cover all states of $\alpha_3 \cup \alpha_5$.

$\Longrightarrow$ How to be sure that the explored POSETs cover the deadlock markings?

# POR techniques: Limitations of POSETs

To cover the deadlock markings of the TPN, it suffices that:

- $\mu$ of $\alpha$ satisfies $D0$, $D1w$, $D2'$ and, in addition, sc: $\forall t \in Fr(\alpha), t \in \mu \Rightarrow (({}^\bullet t)^\bullet \cup (t^\bullet)^\bullet \cup {}^\bullet({}^\bullet t)) \subseteq \mu$ (the transitions that may affect the effect of $t$) [Boucheneb et al. 2015].
- This selection can be limited to the transitions of $(({}^\bullet t)^\bullet \cup (t^\bullet)^\bullet \cup {}^\bullet({}^\bullet t))$ that may occur before $t$ [Boucheneb et. al 2018].




- $\mu = \{t_2\} \models D0 \wedge D1w \wedge D2'$ for $\alpha_0$.
- With sc, $\mu = \{t_2, t_5, t_7, t_4, t_6, t_1, t_3\}$

$\Longrightarrow$ $Fr(\alpha_0) = \mu \cap Fr(\alpha_0)$.

- sc may offset the benefits of the POR techniques, even for conflict-free TPN.

$\Longrightarrow$ Is there a subclass of TPN where POR techniques can be applied without resorting to the POSETs?

# POR techniques without POSETs for a subclass of TPN

- Let $\mathcal{TPN}$ be the set of TPN $\mathcal{N} = (P, T, pre, post, M_0, Is)$ such that $\forall \alpha = (M, F) \in C, \forall t_i \in Fr(\alpha)$,
  - $\uparrow Is(t_i) = \infty \vee$
  - $\forall t_j \in CFS(t_i), t_j \in En(M) \wedge (F \wedge \underline{t}_j \leq \underline{t}_i$ is consistent).

**Theorem**

*Let $\mathcal{N} \in \mathcal{TPN}$. The selective search w.r.t. $D0$, $D1w$ and $D2'$ from the initial state class of $\mathcal{N}$[a] preserves the deadlock markings of $\mathcal{N}$.*

[a] A selective search w.r.t. $D0, D1w$ and $D2'$, from the initial state class of $\mathcal{N}$, is a partial state space exploration, where the set of transitions selected to be fired, from the initial state class and each computed state class, satisfies $D0, D1w$ and $D2'$.

# POR techniques without POSETs for a subclass of TPN

- $\mathcal{TPN} \supset$ Conflict-free TPN i.e., TPN sucht that $\forall t \in T, CFS(t) = \{t\}$.
- $\mathcal{TPN} \supset$ Free-choice TPN i.e., safe TPN such that $\forall t \in T, \forall t' \in CFS(t), pre(t) = pre(t') \wedge \uparrow Is(t) = \uparrow Is(t')$.
- $\mathcal{TPN} \supset$ Weighted comparable preset TPN i.e., safe TPN such that $\forall t \in T, \forall t' \in CFS(t)$,
  - $pre(t) \leq pre(t') \vee pre(t') \leq pre(t))$ and
  - $pre(t) \leq pre(t') \Rightarrow \downarrow Is(t) \leq \uparrow Is(t') \wedge \uparrow Is(t) = \infty$.
- $\mathcal{TPN} \supset$ TPN such that $\forall t \in T, |CFS(t)| > 1 \Rightarrow \uparrow Is(t) = \infty$.

# Conclusion

- This paper discusses the limitations of using the POR techniques in combination with POSETs, in the context of TPN.
- It provides a subclass of TPN that takes advantage of the POR techniques of PN, without resorting to POSETs.
- As future work, we will investigate the expansion of this subclass as well as sufficient structural membership conditions.

# Thank you!